Interference 8 updated Search 4/2

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"digital signature".clm. and certificate.clm. and digest.clm. and computers.clm. and requests.clm. and acknowledgment.clm. and "public key".clm. and valid$4.clm. and generat$4.clm. and pluralit$4. clm. and set.clm. and "d=h".clm.	USPAT	OR	OFF	2006/09/07 12:56
L2	0	"digital signature".clm. and certificate.clm. and digest.clm. and computers.clm. and requests.clm. and acknowledgment.clm. and "public key".clm. and valid$4.clm. and generat$4.clm. and pluralit$4. clm. and set.clm. and "d=h".clm.	US-PGPUB; USPAT	OR	OFF	2006/09/07 12:52
L3	0	"digital signature".clm. and certificate.clm. and digest.clm. and computers.clm. and requests.clm. and acknowledgment.clm. and "public key".clm. and valid$4.clm. and generat$4.clm. and pluralit$4. clm. and set.clm.	US-PGPUB; USPAT	OR	OFF	2006/09/07 12:52
L4	0	"digital signature".clm. and certificate.clm. and digest.clm. and computers.clm. and requests.clm. and acknowledgment.clm. and "public key".clm. and valid$4.clm. and generat$4.clm. and pluralit$4. clm. and set.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/07 12:52
L5	1	"digital signature".clm. and certificate.clm. and digest.clm. and computers.clm. and requests.clm. and "public key".clm. and valid$4. clm. and generat$4.clm. and pluralit$4.clm. and set.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/07 12:53
L6	2811	713/176	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/07 12:53
L7	4422	713/175 or 713/182 or 713/176	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/07 12:55

EAST Search History

L8	8593	713/175 or 713/182 or 713/176 or 283/13 or 382/276 or 705/75 or 713/156 or 714/746	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/07 12:55
L9	66	"digital signature" and certificate and digest and computers and requests and acknowledgment and "public key" and valid$4 and generat$4 and pluralit$4 and set	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/07 12:57
L10	18	8 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/07 12:57

NPL Search - Please Scan

Terms used **digital signature** and **certificate** and **digest** and **computers** and **requests** and **acknowledgment** and **public key** and **valid$4** and **generat$4** and **pluralit$4** and **set**

Found **15,483** of **185,030**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Practical byzantine fault tolerance and proactive recovery

Miguel Castro, Barbara Liskov

November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

Publisher: ACM Press

Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

2 Role-based access control on the web

Joon S. Park, Ravi Sandhu, Gail-Joon Ahn

February 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 1

Publisher: ACM Press

Full text available: pdf(331.03 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Current approaches to access control on the Web servers do not scale to enterprise-wide systems because they are mostly based on individual user identities. Hence we were motivated by the need to manage and enforce the strong and efficient RBAC access control technology in large-scale Web environments. To satisfy this requirement, we identify two different architectures for RBAC on the Web, called user-pull and server-pull. To demonstrate feasibility, we im ...

Keywords: WWW security, cookies, digital certificates, role-based access control

3 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure

Albert Levi, M. Ufuk Caglayan, Cetin K. Koc

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

4 A security architecture for fault-tolerant systems

Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse

November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4

Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

5 A secure and private system for subscription-based remote services

Pino Persiano, Ivan Visconti

November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4

Publisher: ACM Press

Full text available: pdf(241.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper we study privacy issues regarding the use of the SSL/TLS protocol and X.509 certificates. Our main attention is placed on subscription-based remote services (e.g., subscription to newspapers and databases) where the service manager charges a flat fee for a period of time independent of the actual number of times the service is requested.We start by pointing out that restricting the access to such services by using X.509 certificates and the SSL/TLS protocol, while preserving the in ...

Keywords: Access control, anonymity, cryptographic algorithms and protocols, privacy, world-wide web

6 Technical papers: Tradeoffs in certificate revocation schemes

Peifang Zheng

April 2003 **ACM SIGCOMM Computer Communication Review**, Volume 33 Issue 2
Publisher: ACM Press
Full text available: pdf(217.65 KB) Additional Information: full citation, abstract, references

Cryptographic *certificates* are a powerful tool for security concerned applications where the participants must be authenticated in order to access some resources or commit a transaction. However, due to various reasons, the validity of such certificates can change over time, introducing the risk of an invalid certificate being used to authenticate an entity. Various methods of mitigating this risk have been devised, known broadly as "certificate revocation" schemes. In this paper, we cate ...

7 Certificate-based authorization policy in a PKI environment
Mary R. Thompson, Abdelilah Essiari, Srilekha Mudumbai
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(233.63 KB) Additional Information: full citation, abstract, references, citings, index terms

The major emphasis of public key infrastructure has been to provide a cryptographically secure means of authenticating identities. However, procedures for authorizing the holders of these identities to perform specific actions still need additional research and development. While there are a number of proposed standards for authorization structures and protocols such as KeyNote, SPKI, and SAML based on X.509 or other key-based identities, none have been widely adopted. As part of an effort to us ...

Keywords: Public key infrastructure, XML, digital certificates

8 A secure infrastructure for service discovery and access in pervasive computing
Jeffrey Undercoffer, Filip Perich, Andrej Cedilnik, Lalana Kagal, Anupam Joshi
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(308.34 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is paramount to the success of pervasive computing environments. The system presented in this paper provides a communications and security infrastructure that goes far in advancing the goal of anywhere-anytime computing. Our work securely enables clients to access and utilize services in heterogeneous networks. We provide a service registration and discovery mechanism implemented through a hierarchy of service management. The system is built upon a simplified Public Key Infrastructure t ...

Keywords: distributed services, extensible markup language, pervasive computing, security, smartcards

9 How to securely replicate services
Michael K. Reiter, Kenneth P. Birman
May 1994 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 16 Issue 3
Publisher: ACM Press
Full text available: pdf(1.76 MB) Additional Information: full citation, abstract, references, citings, index terms

We present a method for constructing replicated services that retain their availability and integrity despite several servers and clients being corrupted by an intruder, in addition to others failing benignly. We also address the issue of maintaining a causal order among

client requests. We illustrate a security breach resulting from an intruder's ability to effect a violation of causality in the sequence of requests processed by the service and propose an approach to counter this attack. A ...

Keywords: causality, replication, state machines, threshold cryptography

10 Secure group communications using key graphs

Chung Kei Wong, Mohamed Gouda, Simon S. Lam

February 2000 **IEEE/ACM Transactions on Networking (TON)**, Volume 8 Issue 1

Publisher: IEEE Press

Full text available: pdf(345.54 KB) Additional Information: full citation, references, citings, index terms, review

Keywords: confidentiality, group communications, group key management, key distribution, multicast, privacy, rekeying, security

11 Some facets of complexity theory and cryptography: A five-lecture tutorial

Jörg Rothe

December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

12 Authentication in the Taos operating system

Edward Wobber, Martín Abadi, Michael Burrows, Butler Lampson

February 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 1

Publisher: ACM Press

Full text available: pdf(1.88 MB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe a design for security in a distributed system and its implementation. In our design, applications gain access to security services through a narrow interface. This interface provides a notion of identity that includes simple principals, groups, roles, and delegations. A new operating system component manages principals, credentials, and secure channels. It checks credentials according to the formal rules of a logic of authentication. Our implementation is efficient enough to sup ...

Keywords: cryptography, mathematical logic

13 Revising old friends: Separating agreement from execution for byzantine fault tolerant

services
Jian Yin, Jean-Philippe Martin, Arun Venkataramani, Lorenzo Alvisi, Mike Dahlin
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Publisher: ACM Press
Full text available: pdf(355.08 KB) Additional Information: full citation, abstract, references, index terms

We describe a new architecture for Byzantine fault tolerant state machine replication that separates *agreement* that orders requests from *execution* that processes requests. This separation yields two fundamental and practically significant advantages over previous architectures. First, it reduces replication costs because the new architecture can tolerate faults in up to half of the state machine replicas that execute requests. Previous systems can tolerate faults in at most a third ...

Keywords: byzantine fault tolerance, confidentialiy, reliability, security, state machine replication, trustworthy systems

14 Attribute certification: an enabling technology for delegation and role-based controls in distributed environments
John Linn, Magnus Nyström
October 1999 **Proceedings of the fourth ACM workshop on Role-based access control**
Publisher: ACM Press
Full text available: pdf(1.04 MB) Additional Information: full citation, references, citings, index terms

15 Flexible control of downloaded executable content
Trent Jaeger, Atul Prakash, Jochen Liedtke, Nayeem Islam
May 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 2
Publisher: ACM Press
Full text available: pdf(297.79 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a security architecture that enables system and application a ccess control requirements to be enforced on applications composed from downloaded executable content. Downloaded executable content consists of messages downloaded from remote hosts that contain executables that run, upon receipt, on the downloading principal's machine. Unless restricted, this content can perform malicious actions, including accessing its downloading principal's private data and sending messages on th ...

Keywords: access control models, authentication, autorization machanisms, collaborative systems, role-based access control

16 SPV: secure path vector routing for securing BGP
Yih-Chun Hu, Adrian Perrig, Marvin Sirbu
August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4
Publisher: ACM Press
Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of

BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

17 AReCA: a highly attack resilient certification authority

Jiwu Jing, Peng Liu, Dengguo Feng, Ji Xiang, Neng Gao, Jingqiang Lin

October 2003 **Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems: in association with 10th ACM Conference on Computer and Communications Security**

Publisher: ACM Press

Full text available: pdf(1.40 MB) Additional Information: full citation, abstract, references, index terms

Certification Authorities (CA) are a critical component of a PKI. All the certificates issued by a CA will become invalid when the (signing) private key of the CA is compromised. Hence it is a very important issue to protect the private key of an online CA. ARECA systems, built on top of threshold cryptography, ensure the security of a CA through a series of defense-in-depth protections. ARECA systems won't be compromised when a few system components are compromised or some system administrat ...

Keywords: CA, RSA, attack resilience, digital signature, intrusion tolerance

18 General storage protection techniques: Securing distributed storage: challenges, techniques, and systems

Vishal Kher, Yongdae Kim

November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**

Publisher: ACM Press

Full text available: pdf(294.61 KB) Additional Information: full citation, abstract, references, index terms

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

19 Revokable and versatile electronic money (extended abstract)

Markus Jakobsson, Moti Yung

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

20 Password Management and Digital Signatures: The BiBa one-time signature and broadcast authentication protocol

Adrian Perrig

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Publisher: ACM Press

Full text available: pdf(268.66 KB) Additional Information: full citation, abstract, references, citings, index terms

We introduce the *BiBa signature* scheme, a new signature construction that uses one-way functions without trapdoors. BiBa features a low verification overhead and a relatively small signature size. In comparison to other one-way function based signature schemes, BiBa has smaller signatures and is at least twice as fast to verify (which probably makes it one of the fastest signature scheme to date for verification). On the downside, the BiBa public key is large, and the signature generation ...

Keywords: broadcast authentication, one-time signature, signature based on a one-way function without trapdoor, source authentication for multicast

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next